Deutscher Bundestag **Drucksache 17/7104**

17. Wahlperiode 25. 10. 2011

Kleine Anfrage

der Abgeordneten Jan Korte, Andrej Hunko, Ulla Jelpke, Petra Pau, Jens Petermann, Frank Tempel, Halina Wawzyniak und der Fraktion DIE LINKE.

Auskunft über Einsatz staatlicher Schadprogramme zur Computerspionage („Staatstrojaner“)

Am 8. Oktober 2011 veröffentlichte der Hamburger Chaos Computer Club e. V. (CCC) eine 20-seitige Analyse eines ihm in mehrfacher Ausführung zugespielten Schadprogrammes zur Computerspionage (www.ccc.de/de/updates/2011/staatstrojaner). Der CCC kommt zu dem Schluss, dass es sich bei den ihm zugesendeten Trojanern um eine staatliche Software handele, mit der Ermittlungsbehörden die Computer von Verdächtigen ausspähen können.

Die Analyse der extrahierten Binärdateien der Software mache deutlich, dass die Trojaner unter anderem in der Lage seien, weitere Software über das Internet nachzuladen, darunter auch Programme, die eine gegebenenfalls am Zielrechner installierte Webcam zur Raumüberwachung nutzen könnten. Außerdem könnten die Trojaner Programmteile verändern, nicht gesendete E-Mails kopieren und vor allem Dateien auf dem Rechner unbemerkt und ohne Spuren zu hinterlassen, hinterlegen. Damit wären die technischen Möglichkeiten des Programms, also umfängliche Manipulationen an dem Zielrechner vorzunehmen, für staatliche Stellen verfassungswidrig, da die Funktionalität der Software weit über die Grenzen dessen hinaus geht, was das Bundesverfassungsgericht (BVerfG) in seinem Urteil im Jahre 2008 (www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html) vorgegeben hat. Hinzu kommt, dass der Trojaner aufgrund seiner „schlampigen Programmierung“ laut CCC weitere massive Sicherheitslücken enthält. Problematisch bei der Software, sei nach Angaben des CCC der Umstand, dass die ausgespähten Daten zur Verschleierung der Steuerzentrale für die Überwachung über einen „command-and-control“-Server (C+C) in den USA umgeleitet wurden. So könnten Daten ohne großen Aufwand von amerikanischen Dienststellen mitgelesen werden, denn alle US-IT-Firmen sind zur Kooperation mit diesen und entsprechenden Herausgabe der Daten gesetzlich verpflichtet.

Das Bundesministerium des Innern (BMI) widersprach am 9. Oktober 2011 Aussagen, dass es sich bei der Schadsoftware um „Bundes-Trojaner“ handele, die auch von Behörden der Bundesregierung eingesetzt worden seien: „Das Bundeskriminalamt hat den sogenannten Trojaner nicht eingesetzt.“ Und weiter: „Im Übrigen sind die zuständigen Justiz- und Sicherheitsbehörden des Bundes und der Länder jeweils eigenständig für die Einhaltung technischer und rechtlicher Vorgaben verantwortlich.“ Die Bundesministerin der Justiz, Sabine Leutheusser-Schnarrenberger, hat angesichts der Vorwürfe des angeblichen Bundestrojaners „totale Transparenz und Aufklärung“ versprochen. Sie werde auf Bundes- und Länderebene prüfen, ob solch eine Überwachung in Deutschland zum Einsatz komme. Im ARD-„Morgenmagazin“ erklärte die FDP-Politi-

kerin am 10. Oktober 2011: „Wenn das so wäre, wäre es nicht im Einklang mit unseren Gesetzen“, dann müssten geeignete Wege gefunden werden, das zu untersagen. Der Vorsitzende des Innenausschusses des Deutschen Bundestages, Wolfgang Bosbach (CDU), gab gegenüber den Medien zu, dass einigen Mitgliedern des Innenausschusses einmal eine Software vorgeführt worden sei, die die vom CCC beschriebenen Fähigkeiten aufweise. „Man sei sich deswegen im Ausschuss schnell einig gewesen, dass diese Software nicht angeschafft werde“ (vgl. Süddeutsche Zeitung vom 10. Oktober 2011). Aus dem Zeitungsbericht war allerdings nicht ersichtlich, ob der exklusive Kreis einzelner Mitglieder des Innenausschusses daraufhin den Hersteller der Software auf die Illegalität eines Einsatzes der beworbenen Software in der Bundesrepublik Deutschland hingewiesen hatte.

Mittlerweile haben sich Vermutungen bestätigt, dass mindestens einer der Trojaner aus Bayern stammt (vgl. heise online vom 10. Oktober 2011) und dort bereits mehrfach in Ermittlungsverfahren eingesetzt wurde. Am 10. Oktober 2011 gab der Minister des Bayerischen Staatsministeriums des Innern Joachim Herrmann bekannt, die vom CCC analysierte Software stehe in Zusammenhang mit einem Ermittlungsverfahren im Jahr 2009. Die 4. Strafkammer des Landgerichts Landshut hat in ihrem Beschluss vom 25. Januar 2011 den Einsatz dieses „Bayerntrojaners“ für rechtswidrig erklärt.

Programmiert wurde die Software von der privaten hessischen Firma DigiTask (www.digitask.de/).

Laut Angaben der jeweiligen Innenminister wurden Trojaner von den Ermittlungsbehörden der Länder Niedersachsen, Rheinland-Pfalz, Bayern, Brandenburg und Bremen eingesetzt. Während die Innenministerien von Sachsen und Hessen zunächst nicht auf Anfragen des „SPIEGEL“ reagierten, kündigte das Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen an, Erkundigungen einzuleiten, um herauszufinden ob Trojaner in Nordrhein-Westfalen bereits zum Einsatz kamen (vgl. DER SPIEGEL vom 10. Oktober 2011). Das Bundeskriminalamt (BKA) prüft unterdessen, ob weitere Landesbehörden Trojaner eingesetzt haben (vgl. Reuters vom 10. Oktober 2011). Am 10. Oktober 2011 stoppte Baden-Württemberg den Einsatz der Software. Der Innenminister des Landes Baden-Württemberg Reinhold Gall (SPD) räumte ein, bis zu diesem Zeitpunkt sei von der baden-württembergischen Polizei dieselbe Basisversion des Trojaners wie in Bayern verwendet worden.

Behauptet wird, bei anderen Behörden sei andere Schnüffelsoftware im Einsatz als der vom CCC untersuchte Staatstrojaner, den die Firma DigiTask nach eigenen Angaben im November 2008 an das Bayerische Landeskriminalamt lieferte. Der Geheimdienstkoordinator im Bundeskanzleramt wird inzwischen aber damit zitiert, dass die Landesbehörden multifunktionale Rohlinge erhalten hätten, die als Prototypen weit mehr Fähigkeiten als rechtlich zugelassen besäßen und die dann von den Ermittlern auf die jeweils vom Gericht zugelassenen Funktionen reduziert werden sollten (vgl. dpa-Meldung vom 13. Oktober 2011). Die Firma DigiTask, die entsprechende Software zur Telekommunikationsüberwachung in die Niederlande, nach Österreich, in die Schweiz und in Deutschland an „Ermittlungsbehörden auf Landes- und Bundesebene“ verkauft, dürfte mit öffentlichen Aufträgen in den vergangenen Jahren Millionen von Euro umgesetzt haben (vgl. SPIEGEL ONLINE vom 11. Oktober 2011). Nach Angaben des „SPIEGEL“ verlautete aus „Berliner Sicherheitskreisen“, dass das Bundeskriminalamt ebenfalls Software der Firma DigiTask einsetzt – allerdings angeblich nur in modifizierter Version. „Experten hätten die auch von Bayern eingesetzte Version begutachtet und für zu weitgehend befunden. DigiTask habe seine Software nach den Vorgaben von BKA und Bundesinnenministerium angepasst.“ (SPIEGEL ONLINE von 12. Oktober 2011).

Das Bundesministerium der Finanzen teilte unterdessen mit, dass die Zollbehörden in bislang 16 Fällen Spionageprogramme eingesetzt hätten, deren Einsatz aber sei „in einem engen rechtlichen Rahmen und nur zur Überwachung von verschlüsselten Telefonaten“ erfolgt (Frankfurter Allgemeine Zeitung vom 13. Oktober 2011). Im Amtsblatt der Europäischen Union gab das Zollkriminalamt für die Jahre 2008 und 2009 mehrere Aufträge zur Lieferung von Hard- und Software zur Telekommunikationsüberwachung bekannt: 2008 seien demnach für insgesamt 760 000 Euro zwei Aufträge über „TKÜ Auswerte -SW“ und „TKÜ Auswerte Hardware u. Softwarelizenzen“ an die Firma DigiTask vergeben worden (Amtsblatt der Europäischen Union vom 14. März 2008). 2009 folgte ein weiterer Auftrag über 2,1 Mio. Euro ebenfalls an die Firma DigiTask für die „Lieferung von Hard- und Software zur Telekommunikationsüberwachung (TKÜ)“ (Amtsblatt der Europäischen Union vom 29. Januar 2009). Die Firma DigiTask erhielt ferner den Zuschlag durch das Zollkriminalamt für den Auftrag zur „Hardware-Instandhaltungs- und Software-Pflegeleistungen an stationären Telekommunikationsüberwachungsanlagen“ über 700 000 Euro (Amtsblatt der Europäischen Union vom 23. Januar 2009).

Am 19. Oktober 2011 berichtete der „SPIEGEL“, dass der Anti-Viren-Software-Hersteller Kaspersky nach eigenen Angaben eine weitere Version des Staatstrojaners analysiert und dabei festgestellt habe, das das offenbar ebenfalls von der Firma DigiTask entwickelte Programm weitaus mehr Programme abhören kann, als der vom CCC identifizierte Bayern-Trojaner. Auch neuere Betriebssysteme soll der Schädling infizieren können (SPIEGEL ONLINE von 19. Oktober 2011).

Nachdem die Bundesregierung am 21. Mai 2010 in ihrer Antwort auf eine entsprechende Kleine Anfrage der Fraktion DIE LINKE. (Bundestagsdrucksache 17/1814) angab, dass bis Mai 2010 keine einzige Onlinedurchsuchung durch das Bundeskriminalamt vorgenommen worden sei, verweigerte die Bundesregierung in ihrer Antwort am 7. Juni 2011 auf die Kleine Anfrage „Anwendung von Onlinedurchsuchungen“ (Bundestagsdrucksache 17/6079) jegliche Information über die Anzahl durchgeführter Onlinedurchsuchungen, da dies eine „Offenlegung sensibler polizeilicher Vorgehensweisen und Taktiken” der Gefahrenermittlungen des BKA oder des Bundesnachrichtendienstes (BND) darstellen würde.

Inzwischen wurde offenkundig, dass mit ERA IT SOLUTIONS AG auch eine schweizer Firma in den Skandal um die ausufernde Nutzung staatlicher Trojaner-Programme involviert ist. Der Minister für Inneres und Kommunales des Landes Nordrhein-Westfalen hatte etwa zugegeben, dass das Land auch Software des schweizer Unternehmens für Quellen-TKÜ nutzt (Presseinformation vom 13. Oktober 2011). Die Software der Firma DigiTask wurde indes laut einem Bericht der „Neuen Zürcher Zeitung“ vom 15. Oktober 2011 genutzt, um schweizer Computer zu infiltrieren: Demnach stellte die schweizerische Bundeskriminalpolizei ein Rechtshilfegesuch an deutsche Behörden, damit diese den Mail-Verkehr und die Telefongespräche einer Züricher Linksaktivistin abhören. Hierfür wurde von der Firma DigiTask angeblich ein „Mietgerät mit Spezialsoftware“ für 26 000 Euro überlassen. Das Attackieren ausländischer Rechner mit deutschen Trojanern war bislang nur vom Auslandsgeheimdienst BND bekannt, der gemäß dem Nachrichtenmagazin „FOCUS“ vom 29. März 2009 in 90 Fällen Computer in Afghanistan und im Kongo infiltrierte. Grenzüberschreitende Einsätze von staatlichen Trojanern stellen einen Eingriff in die Hoheitsrechte anderer Regierungen dar.

Mit der Überprüfung der vom CCC aufgedeckten Verwendung mindestens eines Trojaners, der verfassungswidrige Eingriffe in den privaten Kernbereich von überwachten Personen ermöglicht und bei dem es sich technisch um eine Onlinedurchsuchung handelt, will die Bundesregierung nach offiziellen Verlautbarungen anscheinend offener umgehen. Die Bundeskanzlerin Dr. Angela

Merkel erklärte, sie würde sich zu den laufenden Ermittlungen auf dem Laufenden halten lassen, auch das BKA werde die Verwendung von Schadprogrammen in den Ländern überprüfen (Reuters, 10. Oktober 2011). Das BKA bestätigte zudem, es habe schon bei der Programmierung der Software zwischen BKA und Landeskriminalämtern einen „Austausch auf Expertenebene" gegeben (zeit.de vom 12. Oktober 2011). Und nicht zuletzt hat die Bundesministerin Sabine Leutheusser-Schnarrenberger Transparenz im Umgang bei der Aufarbeitung des Skandals zugesagt. Wenn diese Zusagen eingehalten wurden, kann also davon ausgegangen werden, dass die Bundesregierung mittlerweile über ausreichendes Wissen über die Vorgänge in den Ländern und in den eigenen Behörden besitzt, um die folgenden Fragen zu beantworten.

Wir fragen die Bundesregierung:

I. Fragen zum vom CCC analysierten Staatstrojaner

1. In wie vielen Fällen wurde die vom CCC analysierte Überwachungssoftware durch Sicherheitsbehörden des Bundes und der Länder bislang eingesetzt (bitte einzeln aufschlüsseln nach jeweiliger Behörde, Anlass für den Einsatz, konkretem Straftatverdacht, Rechtsgrundlage der Maßnahme, Anzahl der betroffenen Personen, Zeitpunkt und Dauer der Überwachungsmaßnahme, konkrete Einsatzfunktion – Kommunikationsüberwachung, Ausspähung und/oder Kopieren privater Daten (Speicherzugriff), Nachladen von Programmen, Kontrolle über den Rechner, Raumüberwachung usw.)?

2. Bei welchen Bundesbehörden wird Trojaner-Software eingesetzt, die im Wesentlichen dem Quellcode des vom CCC analysierten Schadprogramms entspricht bzw. auf einem ähnlichen Installer basiert?

3. Wer gab wann wem den Auftrag zur Entwicklung der vom CCC analysierten Schadsoftware?

4. Wann wurde die Schadsoftware von wem angeschafft, wie hoch waren die Kosten dafür, und wie viele Versionen existierten bzw. existieren davon?

5. Wer gab die Entwicklung weiterer softwarespezifischer Funktionen, z. B. Nachladen weiterer Programme, Zugriff auf Festplatten und den darauf gespeicherten Datenbestand, Kontrolle über den Rechner, Möglichkeiten zur Nutzung der Hardware zur akustischen Raumüberwachung usw., aus welchen Gründen, und auf welcher Rechtsgrundlage in Auftrag?

6. Inwiefern wurde Überwachungssoftware, die von Bundesbehörden genutzt wird, in jedem Einzelfall auf die Einhaltung der Vorgaben aus der Entscheidung des Bundesverfassungsgerichtes zur sogenannten Onlinedurchsuchung geprüft, und wenn ja, mit welchem Ergebnis?

   Aus welchem Grund wurde eine derartige verfassungsrechtliche Prüfung in welchen Fällen unterlassen?

7. Wie wurde die Qualitätssicherung bei der Herstellung, Anwendung sowie Auswertung der jeweils von Bundesbehörden eingesetzten Schadprogramme sichergestellt?

8. Warum wurde bei einem ggf. vorliegenden Verstoß gegen verfassungsrechtliche Vorgaben die Software dennoch erstellt bzw. angeschafft?

9. Hatten die beauftragenden Behörden den Quellcode der jeweils eingesetzten Software vorliegen?

   Wenn nein, warum nicht?

10. War nach Kenntnis der Bundesregierung den beauftragenden Behörden vor dem ersten Einsatz der Software bekannt, dass der Zugriff auf die Software

ohne Authentifizierung stattfindet und auch von nicht autorisierten Personen weitere Software implementiert und zur Ausführung gebracht werden kann, oder wurde die Software mit dieser Funktionalität ohne Auftrag und Wissen der Auftraggeber der Firma DigiTask ausgestattet?

11. Wie ist die Gewährleistung für die Software vertraglich geregelt, und erwägt die Bundesregierung Regressansprüche gegen die Herstellerfirma, für den Fall, dass sich herausstellen sollte, das diese die Verantwortung für den grundgesetzwidrigen Leistungsumfang ihres Produkts trägt (bitte begründen)?

12. Sind nach Kenntnis der Bundesregierung weitere Versionen der Software in Entwicklung, und wenn ja, welche Eigenschaften sollen diese Software-Versionen bekommen?

13. Ist der Einsatz der vom CCC analysierten Software aus Sicht der Bundesregierung angemessen und gerechtfertigt, und wenn ja, in welchen Fällen und auf welcher Rechtsgrundlage?

    Wenn nein, warum nicht und welche Konsequenzen zieht sie daraus?

II. Fragen zum Einsatz von Staatstrojanern allgemein und zur technischen Kontrolle der Schadsoftware

14. Welche Bundesbehörden haben zu welchem genauen Zeitpunkt die Entwicklung, den Kauf oder die Lizenzierung von welcher Softwarelösung mit welchem Leistungsumfang und welcher Funktionalität zur Telekommunikationsüberwachung bei welcher Firma und zu welchen Kosten in Auftrag gegeben?

    Trifft es zu, dass eine „Onlineaktualisierung“, also Code-Nachladen, Bestandteil des Angebots bzw. des Pflichtenheftes war?

15. Trifft es zu, dass es sich bei der vom Anti-Viren-Software-Hersteller, Kaspersky analysierten Software, um den „großen Bruder“ des vom CCC untersuchten Staatstrojaners handelt, und wenn ja, welche Sicherheitsbehörden des Bundes und der Länder verfügen über diese Software?

16. Haben beauftragende Bundesbehörden vor Einsatz von Schadsoftware zum Infiltrieren von Computersystemen vor ihrem Einsatz im Einzelfall den Quellcode geprüft?

    Wenn ja, wie (intern/extern), existieren entsprechende Prüfberichte, wem lagen/liegen diese vor, und welches Ergebnis hatten sie?

17. Wurde hinterher geprüft, dass das eingesetzte Programm tatsächlich aus diesem Source compiled wurde?

    Wenn nein, warum nicht?

18. Wie wurde jeweils sichergestellt, und wer hat die Einhaltung wie kontrolliert, dass die mit der Programmierung der Software beauftragten Firmen entsprechend zertifiziert sind, solche Aufträge durchzuführen?

19. Sahen und sehen die Lasten- und Pflichtenhefte der jeweils beauftragten Firmen vor, ein Sicherheitsaudit der Software durchzuführen, und wenn ja, wurde dieses Audit von einem unabhängigen Unternehmen oder einer anderen Institution durchgeführt, und wenn ja, von wem?

    Wenn nein, warum nicht?

20. Haben die beteiligten Behörden hinreichend qualifizierte Mitarbeiter für ein Source-Audit?

    Wenn ja, um wie viele Personen handelt es sich jeweils (bitte nach Anzahl der Personen und Sicherheitsbehörde auflisten)?

21. Sind Bundesbehörden technisch in der Lage, auch hard- oder softwarebasierte Angriffe auf Mobilfunkgeräte auszuführen?

22. Wie ist die Aussage der Bundesregierung in der Antwort auf die Kleine Anfrage auf Bundestagsdrucksache 17/5677 zu Frage 18 nach „Ferndurchsuchungen“ zu verstehen, wonach das Bundeskriminalamt die „für einen solchen Eingriff erforderlichen und den rechtlichen Voraussetzungen genügenden Einsatzmittel (sog. Remote Forensic Software) entwickelt“ habe, und welche Anwendungen sind hiermit gemeint?

23. In wie vielen Fällen wurde der Einsatz der Überwachungssoftware mit jeweils welchem Funktionsumfang richterlich angeordnet bzw. genehmigt?

24. Gab es jenseits der obligatorischen richterlichen Prüfung im Rahmen des sog. Richtervorbehalts eine Überprüfung der jeweils eingesetzten Überwachungssoftware, und wenn ja, wer führte diese durch (bitte einzeln aufschlüsseln nach jeweiliger Behörde, Anlass für den Einsatz, konkretem Straftatverdacht, Rechtsgrundlage der Maßnahme, Anzahl der betroffenen Personen, Zeitpunkt und Dauer der Überwachungsmaßnahme, konkrete Einsatzfunktion – Kommunikationsüberwachung, Ausspähung und/oder Kopieren privater Daten (Speicherzugriff), Nachladen von Programmen, Kontrolle über den Rechner, Raumüberwachung usw. – und beauftragter Firma)?

25. In wie vielen Fällen wurde eine andere als die vom CCC analysierte Überwachungssoftware durch Sicherheitsbehörden des Bundes und der Länder bislang eingesetzt (bitte einzeln aufschlüsseln nach jeweiliger Behörde, Anlass für den Einsatz, konkretem Straftatverdacht, Rechtsgrundlage der Maßnahme, Anzahl der betroffenen Personen, Zeitpunkt und Dauer der Überwachungsmaßnahme, konkrete Einsatzfunktion – Kommunikationsüberwachung, Ausspähung und/oder Kopieren privater Daten (Speicherzugriff), Nachladen von Programmen, Kontrolle über den Rechner, Raumüberwachung usw. – und beauftragter Firma)?

26. Gab es bei Ermittlungsverfahren, in denen eine sog. Quellen-TKÜ oder eine Onlinedurchsuchung durchgeführt wurde, Amtshilfe zwischen einzelnen Landeskriminalämtern und Bundesbehörden, und wenn ja, in welchen Fällen geschah dies, in welcher Art und Weise (bitte einzeln aufschlüsseln nach jeweiligen Behörden, Anlass für den Einsatz, konkretem Straftatverdacht, Rechtsgrundlage der Maßnahme, Anzahl der betroffenen Personen, Zeitpunkt und Dauer der Überwachungsmaßnahme, verwendeter Software, Art der Amtshilfe)?

27. Wird durch das BKA oder andere Bundes- und Landesbehörden bei Onlinedurchsuchungen die gleiche Basissoftware wie für TKÜ-Maßnahmen (sog. Quellen-TKÜ) benutzt?

    Wenn nein, wer hat die bei Onlinedurchsuchungen verwendete Software entwickelt, wer hat die Software in welchem Rahmen geprüft, und wie viel hat die Entwicklung gekostet?

28. Von wem wurde bzw. wird die entsprechende Überwachungssoftware (Frage 27) installiert und ausgeführt, wie geschah bzw. geschieht dies, und sind dabei auch Hardwareeingriffe am Rechner der überwachten Person notwendig?

29. Waren zur mittelbaren oder unmittelbaren Infektion des Zielrechners mit Überwachungssoftware Absprachen mit Internetdienstleistern notwendig, und wenn ja, in welchen Fällen, mit welcher Software, und mit welchen Telekommunikationsdienstleistern erfolgten diese, und wie waren die jeweiligen Unternehmen in die Überwachungsmaßnahmen involviert?

30. Auf welche Art und Weise wurde Schadsoftware im Einzelfall in betreffende Rechnern eingebracht (bitte jeweils nach etwaigem physischem Eindringen in den Rechner/Wohnung oder manipuliertem Download auflisten)?

31. Wie setzt sich der Trojaner jeweils im System des Zielrechners fest, und welche Dateien sind davon betroffen?

32. Waren und/oder sind Hersteller von Sicherheitssoft- oder -hardware (z. B. Firewalls und Virenscanner) in die Überwachungsmaßnahmen mit eingebunden, und wenn ja, in welcher Form geschieht dies?

33. Über welchen Weg gelangen die Daten vom überwachten Rechner zu den jeweiligen Ermittlungsbehörden, und welche Firmen, Behörden und/oder dritte Personen und Institutionen haben hierbei Zugriff auf die benötigten Server?

34. Hat die Bundesregierung Kenntnis darüber, ob Sicherheitsbehörden in den USA auf die ausgespähten Daten Zugriff gehabt haben, und wenn ja, in wie vielen Fällen geschah dies?

    Wenn nein, wie kann die Bundesregierung dies ausschließen?

35. Wie stellen die Sicherheitsbehörden oder die mit der Überwachung beauftragten Firmen sicher, dass eine Manipulation der Ermittlungen, etwa durch eine auf diesem Übertragungsweg stattfindende Manipulation der Daten durch Dritte, verhindert wird?

36. Wie wurde und wird sichergestellt, dass der Überwachte nach einer möglichen Entdeckung der Software diese oder deren gesammelte Ergebnisse vor der Übersendung an die während der Überwachungsmaßnahme benutzten Server nicht manipulieren oder entfernen kann?

37. Kann sich die von den Sicherheitsbehörden genutzte Software selbstständig innerhalb eines Computernetzwerkes verbreiten, um so Zweit- oder Drittgeräte des Überwachten zu infiltrieren?

38. Wie stellen die Sicherheitsbehörden sicher, dass bei der von ihnen genutzten Überwachungssoftware keine Programme oder Dateien auf das System der überwachten Person übertragen und/oder ausgeführt werden kann?

39. In wie vielen Fällen haben Infektionen mit staatlicher Schadsoftware dabei zum Versagen des Betriebssystems angegriffener Rechner geführt, und wie sind Schadensersatzansprüche hierzu geregelt?

III. Fragen zum möglichen Missbrauch der Staatstrojaner und zum Schutz unbeteiligter Dritter

40. Wie viele Fälle sind der Bundesregierung bekannt, in denen mit der Überwachung betraute Beamte oder Angestellte der damit beauftragten Firmen missbräuchlich an persönliche Daten, die durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschützt sind, gelangt sind?

41. Welche Maßnahmen wurden durch die Sicherheitsbehörden getroffen, die einen solchen Missbrauch unrechtmäßig erlangter Daten der überwachten Personen oder unbeteiligter Dritter verhindern sollen, und inwieweit kann die Bundesregierung ausschließen, dass derartige Daten den Hoheitsbereich der deutschen Strafverfolgung verlassen?

42. In welcher Form und wie lange werden die im Rahmen der Überwachungsmaßnahme ermittelten Daten sowie deren Auswertungsergebnisse gespeichert, stehen diese Daten auch anderen Sicherheitsbehörden zur Verfügung, und wie ist sichergestellt, dass keine Unbefugten Zugriff auf diese Daten bekommen?

43. Wie wurde und wird der Schutz Dritter, die zufällig mit der überwachten Zielperson in Kontakt stehen, gewährleistet, und inwieweit werden diese Personen über die Überwachungsmaßnahme in Kenntnis gesetzt?

44. Auf welcher Rechtsgrundlage wird Betroffenen nach Abschluss der Ermittlungen die Analyse des gegen sie eingesetzten Trojaners zur Überprüfung eventueller Grundrechtsverletzungen verweigert?

IV. Fragen zur Sicherheitsarchitektur

45. Welche informellen Treffen, Arbeitsgruppen oder sonstigen Abstimmungen hat es zum Einsatz von Schadprogrammen zum Eindringen in andere Rechnersysteme auf Ebene von Bund und Ländern gegeben, und welche Arbeitsaufträge sowie Ergebnisse lieferten diese?

46. Kann die Bundesregierung die Aussage des Geheimdienstkoordinators im Bundeskanzleramt bestätigen, dass die Länderbehörden multifunktionale Rohlinge erhalten und diese von den Ermittlern je nach Vorgabe der zuständigen Gerichte in ihren Funktionen reduziert werden, und von welchen Länderbehörden ist hier die Rede?

47. Welche Struktur, einschließlich der personellen Ausstattung zur Bündelung der Telekommunikationsüberwachung des Bundes und der Länder besteht inzwischen beim Bundesverwaltungsamt (BVA), und welche Rolle spielt das BVA bei den aktuellen Vorgängen?

48. Wenn die zur Debatte stehenden Quellen-TKÜ-Maßnahmen nicht in letzter Instanz beim BVA koordiniert und ausgewertet werden, welche Abteilung welcher Bundesbehörde ist dafür zuständig, oder welche Bund-Länder-Arbeitsgruppe wurde zwischen Behörden oder Regierungsstellen oder im Rahmen der Arbeitskreise der Innenministerkonferenz (IMK) eingerichtet?

49. Haben das BKA oder andere Bundesbehörden auch eigene Softwarelösungen zum Einschleusen von Schadsoftware auf Zielrechner oder zur Überwachung der Telekommunikation erarbeitet, und wenn ja, welche Funktionalität haben diese, welche Kosten sind dabei entstanden, wie oft und wann wurde von der Software Gebrauch gemacht?

V. Fragen zum Export und europaweiten Einsatz der Spähsoftware

50. Welche Praxis bzw. Überlegungen für das Ausspähen fremder Rechnersysteme existieren durch die EU-Polizeiagentur Europol, auch hinsichtlich einer Koordinierung von Maßnahmen oder technischer Beratung/Hilfe?

51. Welche Geschäftsbeziehungen hatten Bundesbehörden bislang mit dem schweizer Unternehmen ERA IT SOLUTIONS AG, und welche Vereinbarungen haben sich hieraus ergeben?

52. Stimmt der Pressebericht der „Neuen Zürcher Zeitung“ vom 15. Oktober 2011, wonach die schweizerische Bundeskriminalpolizei ein Rechtshilfegesuch an deutsche Behörden stellte, um „Mail-Verkehr und die Telefongespräche“ einer Züricher Linksaktivistin abzuhören, und falls ja, welche ergänzenden Mitteilungen kann die Bundesregierung hierzu machen?

53. Mit welchen anderen Ländern haben Bundesbehörden Vereinbarungen getroffen, um ausländische Rechner mit deutschen Trojanern zu infiltrieren, und wie wurde dieser Eingriff in die Hoheitsrechte einer anderen Regierung jeweils geregelt?

54. Welche informellen Arbeitsgruppen oder sonstigen Treffen haben hierzu auf internationaler oder EU-Ebene stattgefunden, um grenzüberschreitende Einsätze behördlicher Schadsoftware zu regeln oder zu vereinfachen, und welche Verabredungen wurden dort getroffen?

Wie wird die Bundesregierung den Beschluss des Europäischen Parlaments vom 27. September 2011 umsetzen, wonach Exporte von polizeilicher und nachrichtendienstlicher Überwachungstechnologie in Zukunft strengeren Ausfuhrkriterien unterliegen sollen?

55. Für welche aus Deutschland gelieferten „Abfangtechniken und Vorrichtungen der digitalen Datenübertragung, mit denen Mobiltelefone und Textnachrichten überwacht und die Internet-Nutzung gezielt beobachtet werden können“ kommt der EU-Parlamentsbeschluss nach Ansicht der Bundesregierung infrage?

56. Wie beurteilt die Bundesregierung die Aussage von EU-Parlamentariern (PCWorld, 27. September 2011), wonach vor allem kleine Technologieunternehmen bezüglich kritischer Exporte intransparent sind?

57. Ist der Bundesregierung bekannt, dass zahlreiche deutsche Unternehmen regelmäßig mit Spionagesoftware auf internationalen Verkaufsmessen für Überwachungstechnologie teilnehmen, darunter neben DigiTask auch die Firmen Elaman GmbH, trovicor GmbH, ATIS UHER SA, ipoque GmbH und Utimaco Safeware AG?

58. Wie bewertet es die Bundesregierung, wenn die genannten Unternehmen ähnlich unkontrollierbare Anwendungen wie der vom CCC analysierte Trojaner hierzulande wegen gesetzlicher Hindernisse nicht einsetzen dürfen, jedoch Märkte adressieren, in denen auch die Bundesregierung Menschenrechtsverletzungen durch Polizeien kritisiert?

59. Haben deutsche Behörden jemals mit den Firmen Elaman GmbH, trovicor GmbH, ATIS UHER SA, ipoque GmbH und Utimaco Safeware AG geschäftlich zusammengearbeitet, bzw. hat sich eine der beiden Seiten jemals um eine solche Zusammenarbeit beworben, und falls ja, wann, und in welchen Fällen geschah dies, und welche Verabredungen wurden konkret getroffen?

60. Welche Stelle beim Bundes- bzw. dem Zollkriminalamt ist für testweise Nutzung von Abhör-, Spionage- oder Ermittlungssoftware zuständig?

61. Welche Bundesbehörden nutzen Produkte von der Firma rola Security Solutions GmbH, und um welche Anwendungen handelt es sich konkret bzw. welche Leistungsmerkmale und Schnittstellen zu welchen Datenbanken haben diese?

62. Welche Software nutzen Bundesbehörden zur Auswertung großer Datenmengen aus der Telekommunikationsüberwachung, und wird hierfür auch die Anwendung „Koyote“ von der Firma INTS GmbH genutzt?

    Falls ja, an welche Datenbanken ist diese über Schnittstellen angebunden, und über welche sonstigen Leistungsmerkmale verfügt diese?

63. Welche Software nutzen Bundesbehörden – auch testweise – von der Firma IBM Deutschland Research & Development GmbH, in welchen Feldern werden diese eingesetzt, um welche Anwendungen handelt es sich konkret, und über welche Features verfügen diese?

64. Sind Bundesbehörden jemals geschäftliche Beziehungen – auch testweise – mit den Firmen SPSS inc., humanIT Software GmbH, Inxight, In-Q-Tel oder L-1 Identity Solutions inc. eingegangen, und wenn ja, mit welchem Inhalt?

Berlin, den 25.Oktober 2011

Dr. Gregor Gysi und Fraktion



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333